RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: NCS-M03

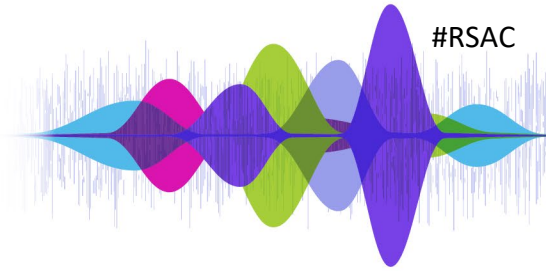
ECH: Hello to Enhanced Privacy or Goodbye to Visibility?

Roelof du Toit

Distinguished Engineer
Enterprise Security Group at Broadcom
www.linkedin.com/in/roelof-du-toit

Arnaud Taddei

Global Security Strategist | ITU-T SG17 Chair
Enterprise Security Group at Broadcom
www.linkedin.com/in/arnaudtaddei



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

30 years ago...

When Netscape Navigator was released strong encryption algorithms were considered munitions and could not be exported, special export restricted installers were produced for the US and Canada.

https://commons.m.wikimedia.org/wiki/File:Netscape_Navigator_1.1_for_Macintosh_Install_Disk.jpg
License: CC BY-SA 4.0
Author: Kevin van Haaren

30 years ago...

This NeXT workstation (a NeXTcube, monitor Cern 57503) was used by Tim Berners-Lee as the first Web server on the World Wide Web.

https://commons.wikimedia.org/wiki/File:First_Web_Server.jpg
License: CC BY-SA 3.0
Author: User:Coolcaesar at en.wikipedia

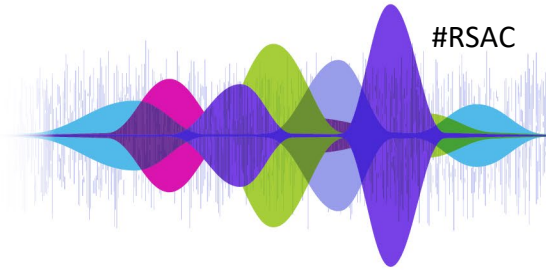
RSAC 2025 Conference

Encrypted Client Hello (ECH)

Technical Background

Many Voices.
One Community.

Encrypted Client Hello in a nutshell



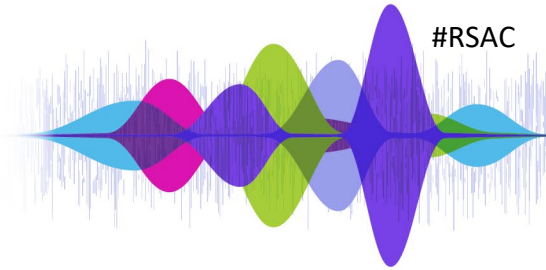
What?

- IETF standard that defines an extension to TLS 1.3.
- Encrypts metadata in the TLS ClientHello message that were previously visible - most notably the destination information represented by the SNI (Server Name Indication).
- Uses DNS to share the encryption keys.

Why?

- Prevents leaking of TLS metadata (SNI, ALPN, etc) to on-path devices.
- Enhances user privacy by protecting sensitive information.
- Optionally allows for deployment of internal origins behind a common public entry point.

Encrypted Client Hello in a nutshell



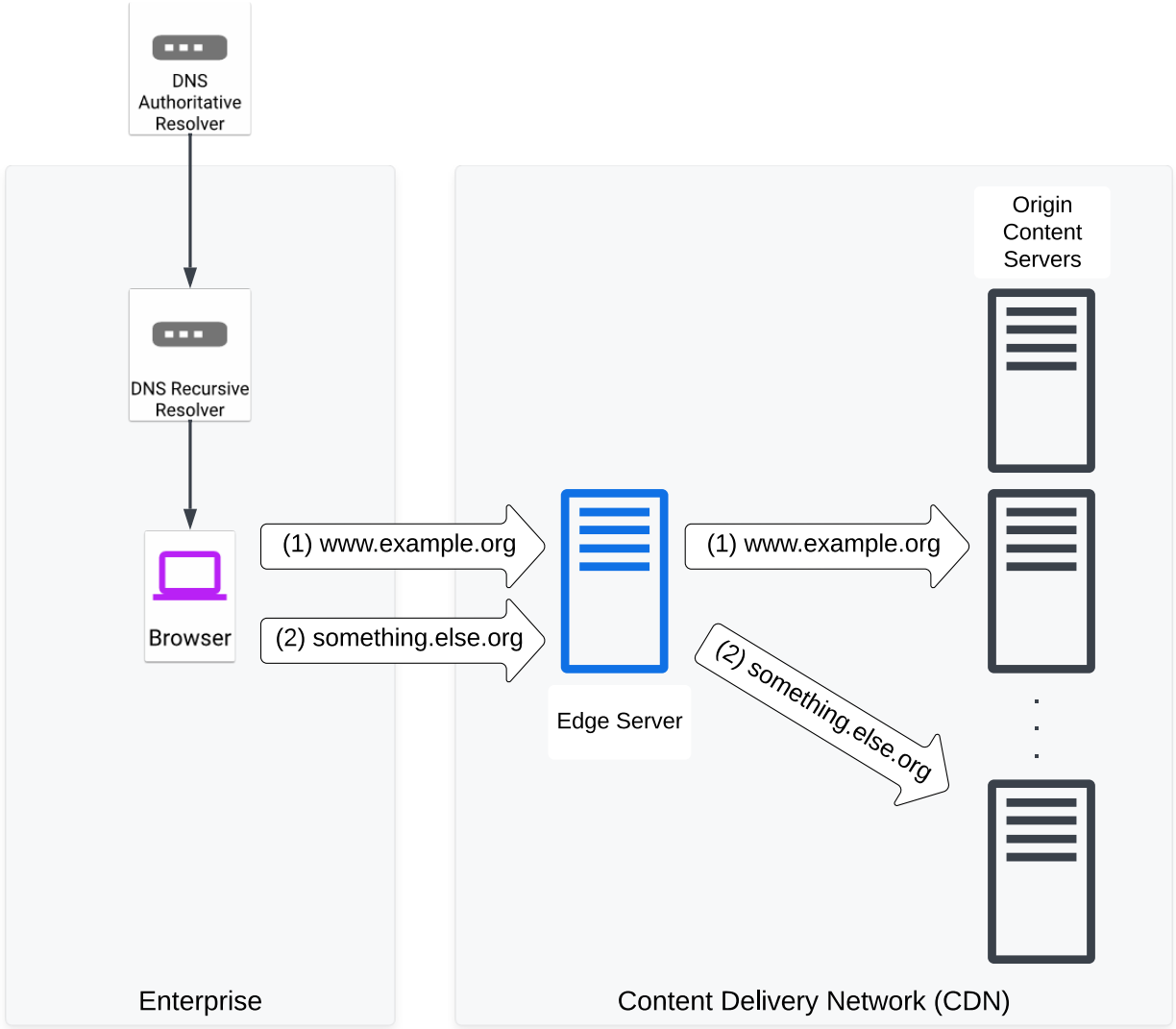
When?

- Already deployed in production.
- Supported by most major browsers, but currently disabled if an explicit proxy is configured.
- Ratification: TBD (draft may get ratified before publication of this presentation)

Who?

- Content Delivery Networks (CDNs)
- Major players: Cloudflare, Fastly, Amazon, Akamai.
- 99.9% of the top 10,000 sites use a CDN[4]

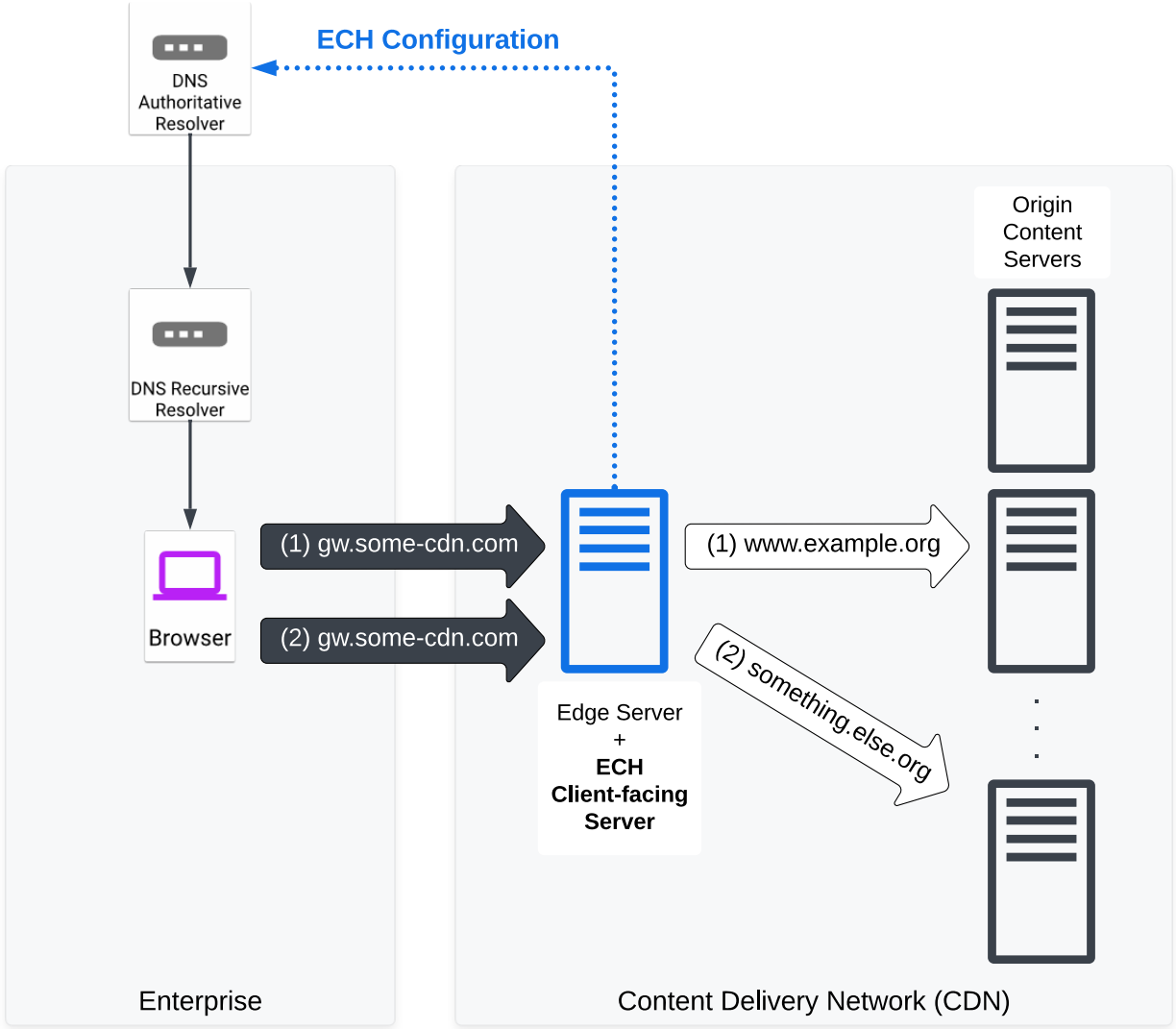
Content Delivery Network access before ECH



Example:

- Some enterprise user loads two unrelated sites from the same browser, and both sites happen to be hosted by the same CDN.
- Logically the origin servers are separated by the CDN.
- Intermediary network devices between the browser and CDN edge server have access to the origin server hostname.

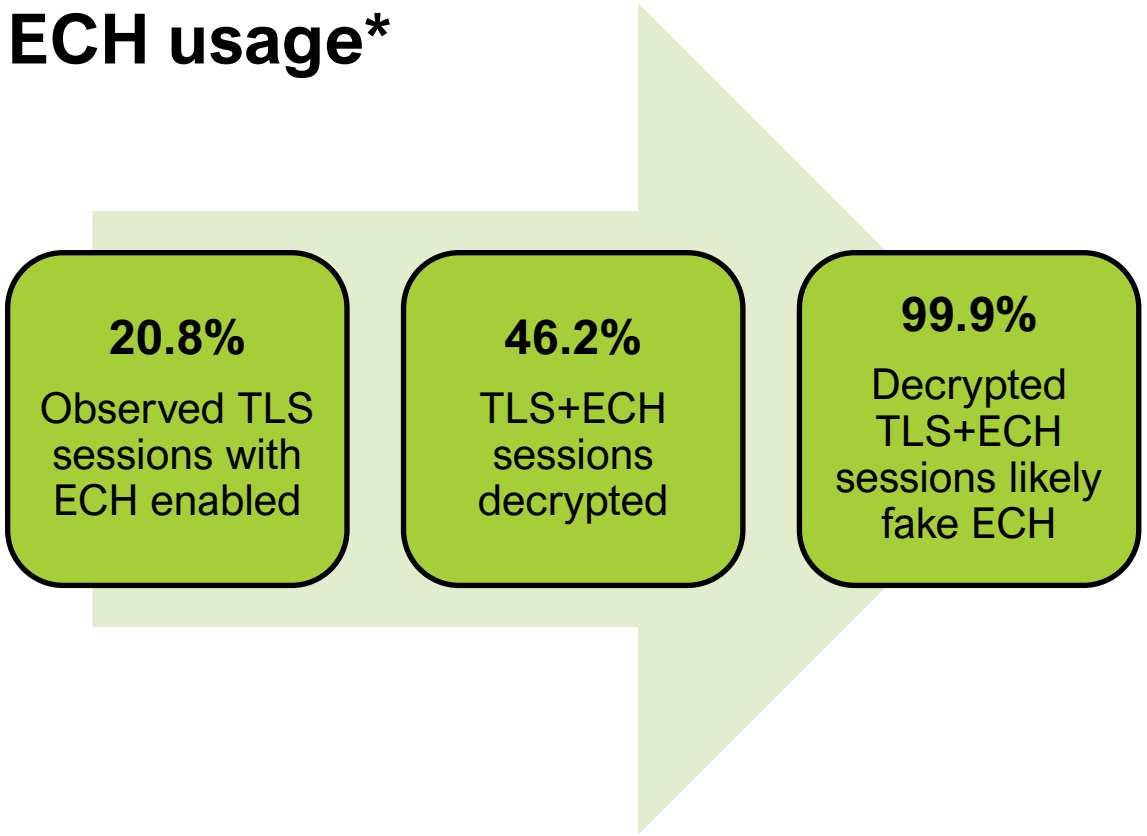
Content Delivery Network access using ECH



- The user loads the same two unrelated sites, both still hosted by the same CDN. The browser uses ECH for the sessions.
- Intermediary network devices between the browser and CDN edge server cannot distinguish between the two sessions. Both sessions seem to have the same destination.
- Only the CDN edge server knows the final origin server for each session. It is acting as ECH client-facing server and can decrypt the encrypted ClientHello to extract the final destination.
- The CDN shares the ECH configuration for those sites through DNS.

ECH usage and deployment numbers

ECH usage*



ECH deployment

- **23.6%** of top 15M sites use a CDN[4]
- **99.9%** of top 10K sites use a CDN[4]
- **70%** of sites using a CDN use Cloudflare[4]
- **9.2%** of top 1M sites* have ECH enabled
- **99.9%** of the ECH-enabled sites use Cloudflare

RSAC 2025 Conference

What is the technical impact of ECH on network security solutions?

Visibility into encrypted traffic while using ECH

Many Voices.
One Community.

Visibility of TLS metadata for network security controls

TLS 1.2

- Target host (SNI)
- Supported application protocols
- Negotiated application protocol
- Session reuse identifiers
- Session reuse confirmation
- Supported cipher-suites
- Negotiated cipher-suite
- Supported algorithms
- Key exchange algorithm
- Advertised TLS extensions
- Negotiated TLS extensions
- Server certificate
- Client certificate (is used)
- TLS record types

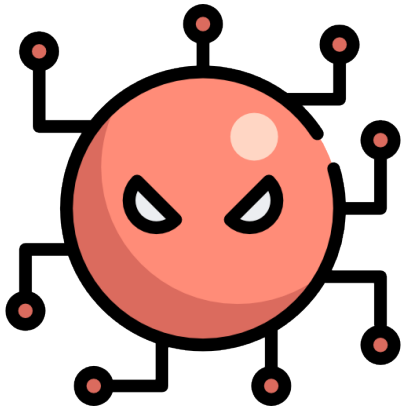
TLS 1.3

- Target host (SNI)
- Supported application protocols
- Supported cipher-suites
- Negotiated cipher-suite
- Key exchange algorithm
- Advertised TLS extensions

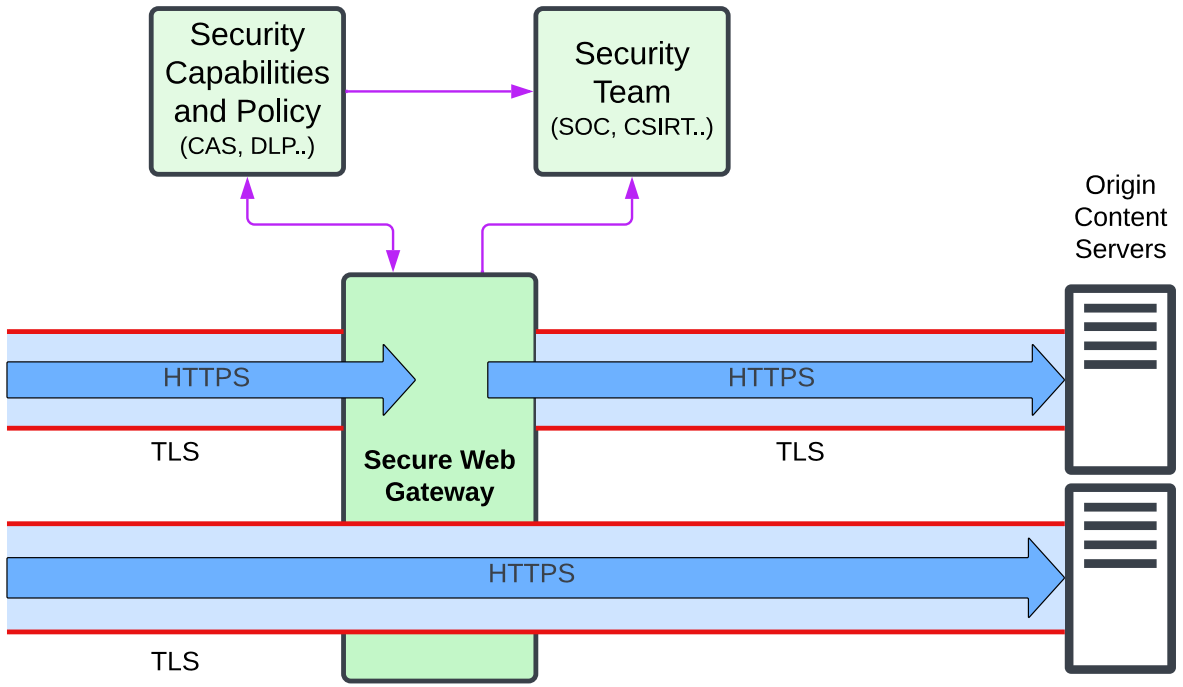
!

TLS 1.3 + ECH

- ECH public name (SNI)
- Negotiated cipher-suite
- Key exchange algorithm

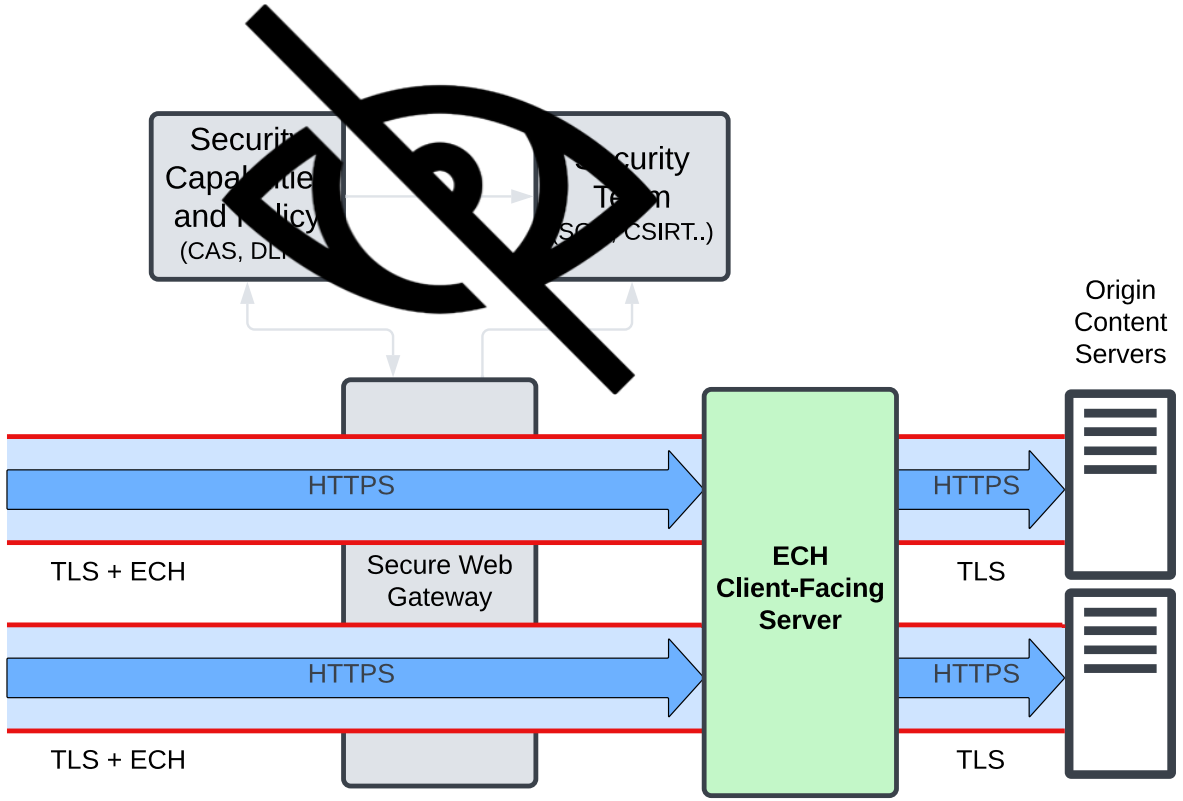


Organizations apply selective TLS decrypt



- Network security policy is based on available metadata.
- Security capabilities are selectively enabled for compliance and privacy
- Security teams depend on security capability incident reporting

Impact of ECH on selective TLS decrypt



- Most of the previously available metadata are hidden when ECH is enabled
- Selective TLS decrypt is no longer feasible
- Security capabilities are blind, and security teams miss important incidents

RSAC 2025 Conference

Why is ECH a game-changer for security?

The impact of ECH on enterprise infrastructure

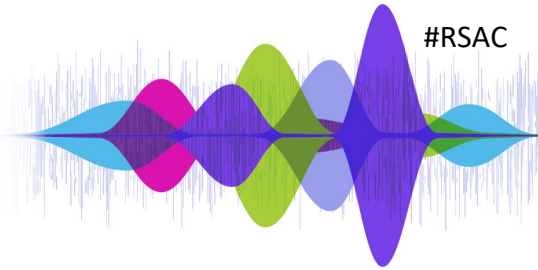
Many Voices.
One Community.

ECH deployment is driving changes to the whole ecosystem

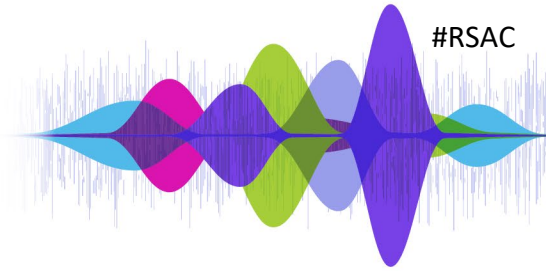
Start	Status	Document	Title
2017	2020	RFC 8744	Issues and requirements for encrypting the TLS SNI
2019	2022	RFC 9180	Hybrid Public Key Encryption
2018	2023	RFC 9460	Service binding and parameter specification via DNS
2020	2023	RFC 9461	Service binding mapping for DNS servers
2020	2023	RFC 9462	Discovery of designated resolvers (DDR)
2020	2023	RFC 9463	DHCP options for discovery of designated resolvers
2018	**R 23***	**draft-ietf-tls-esni**	**TLS Encrypted Client Hello**
2019	Rev 6	draft-ietf-tls-wkech	Well-known URI for publishing service parameters
2019	Rev 8	draft-farrell-tls-pemesni	PEM file format for ECH
2023	Rev 7	draft-ietf-tls-svcb-ech	Bootstrapping ECH with DNS service bindings
2025	Rev 0	draft-sullivan-tls-implicit-ech	Implicit ECH configuration

- IETF standards / Internet Drafts related to ECH
- Adding the history that leads to this ecosystem would make a very large chronogram
- As of writing ECH has not been ratified yet

How is ECH impacting enterprise network security infrastructure?



- Reduced network visibility
  - Network traffic monitoring and incident response
  - Malware detection and prevention
  - Acceptable use policy enforcement
  - Filtering malicious and high risk destinations
  - Data exfiltration detection and prevention
  - Cloud access security broker
- Selective TLS decrypt will no longer be possible
  - Increased compliance risk
  - Increased cost



Conclusion

Network security is now increasingly a system problem instead of a self-contained stack

RSAC 2025 Conference

What are the regulatory and compliance perspectives on ECH?

Considerations the community should take note of

Many Voices.
One Community.

Current Situation

- In the general case
  - Encryption cannot be (easily) broken on communication systems, e.g. http**s**://...
  - Examples: routine residential use cases, access to your bank, etc.
- When it comes to critical infrastructures or government agencies
  - Encrypted traffic **can be an attack vector (ransomware)**
- For an organization to decrypt and inspect its traffic is current standard security operations practice
  - An entire product market encompasses this operations practice
  - It provides valuable intelligence and response capabilities to security teams on threats
  - **Note that it has no relation to the current debate about law enforcement access to encryption**
- Why is decrypting and inspecting an organization's own traffic important?
  - For compliance reasons, e.g. detect data leakage, access to content, analyze incidents
  - For security reasons, e.g. apply malware protection capabilities
- Don't let bad things come in and don't let good things go out

Why are we in this situation?

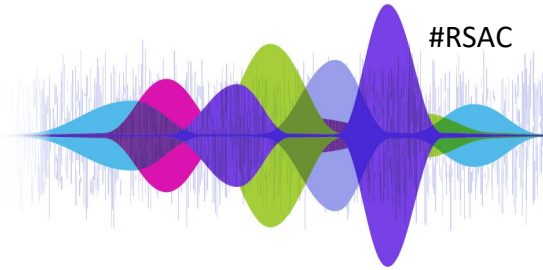
- Post Snowden reaction at IETF
  - 2013: RFC 7258 “Pervasive Monitoring as an Attack”
  - 2025: ECH considers passive and active attackers (middleboxes)

Hardening of “attackers” definition

- On top of “ECH drives the whole ecosystem”, ECH is part of a much bigger context

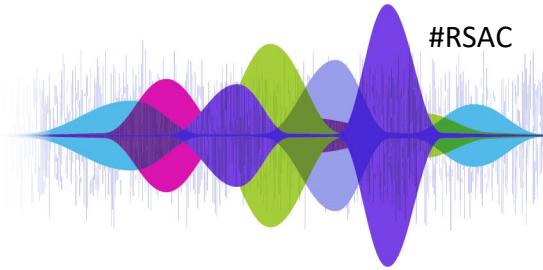
Pervasive Encryption	Last piece of a large puzzle (on top of TLS1.3, DoH, etc.)
DNS Subsystem	Participates to a significant change in the DNS area
Internet Principle	Accelerates the move from End-to-End to an Edge-to-Edge principle Content Deliver Network (CDN) era acceleration
Transport and HTTP	ECH will impact the transport and application layer
Anonymity	More privacy protocols will decrease visibility even further

The intention is to move security from the infrastructure layer to the application layer



- More dimensions are at play
  - QUIC and HTTP/3 move the communication stack outside the kernel on endpoints.
  - Human Rights wants security at content delivery layer (CDN) and not infrastructure layer.
  - Absolute dogma against any form of filtering, not even on the endpoint.

To read the situation requires the introduction of a concept called “Theory of Design”



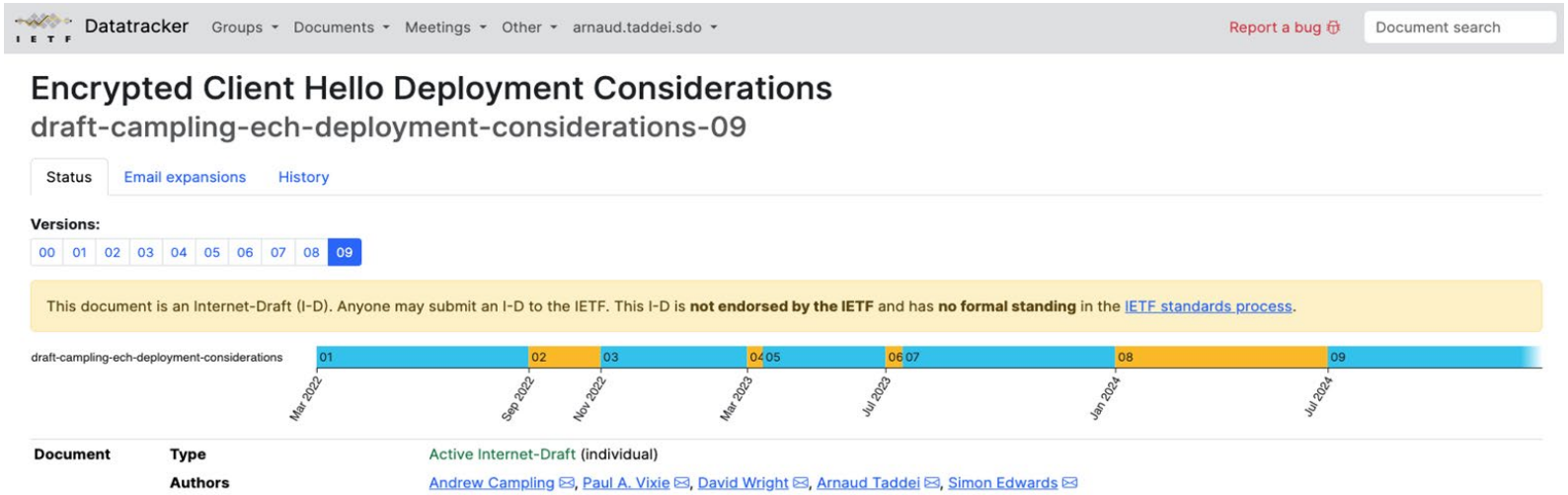
- Need to take a step back and consider higher level requirements in the right (reverse) order

  Technology → Legal → Ethics → Anthropology

- Back to “30 years ago” the world wide web was designed with very different intentions
  - And certainly not using the current very narrow model of individuals
- Would introducing a concept of “sub-contexts” help?
  - Sub-context examples: “Child Online Protection”, “Enterprises”, etc.
  - It would require consensus, investments and migration/transformation costs.

ECH creates a win/lose situation

- IETF draft on ECH Deployment Considerations[3]



Authors

Andrew Campling

Paul Vixie

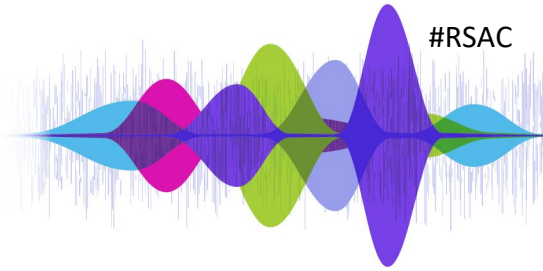
David Wright

Arnaud Taddei

Simon Edwards (RIP)

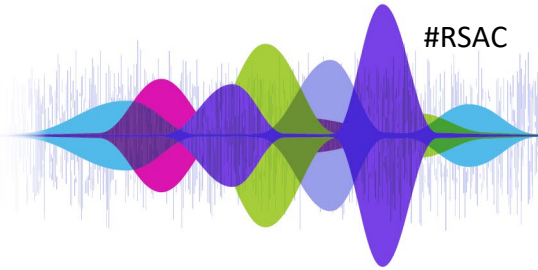
- Identification of four initial use cases which will face unanticipated issues
  - Child Online Protection
  - Education
  - Public Networks
  - Enterprise

Implications for national and regional administrations



- Impacts threat intelligence capabilities and regulatory requirements
  - National and regional administrations threat intelligence sharing requirements will be under pressure
  - Organizations self defense will be impacted
  - This is as well creating a massive resilience issue and sovereignty one too
  - This is not a vendor technological problem
  - This is discussed among select players (CDNs, Browser Makers, Human Rights, Critical Infrastructure, etc.)
  - This is a security operations and threat intelligence problem
  - This is not a law enforcement problem

Some suggestions for administrations

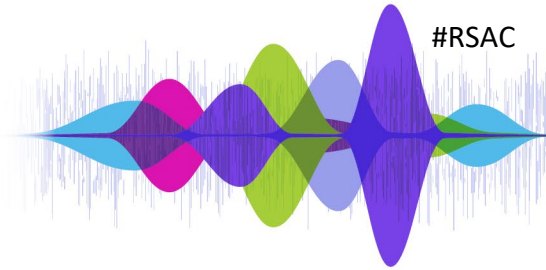


- Study the problem in full depth
- Consider the impact to your policy objectives and on existing and forthcoming regulatory implementations
- Consider the impact for all regional constituencies
  - Member states
  - Critical infrastructure
  - Specific sectors, e.g. financial entities
- Consider the impact beyond security
  - Resilience, centralization, trustworthiness, sovereignty, etc.

RSAC 2025 Conference

Summary

Apply what you have learned in the next few weeks

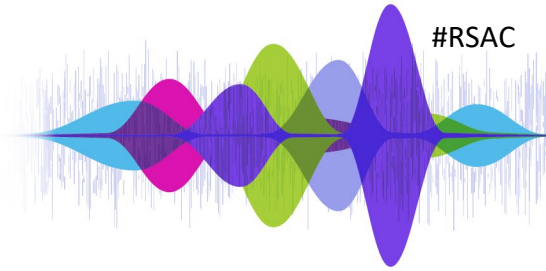


In the next few weeks you should:

- Form a strategic initiative at CISO executive level.

  Align internal stakeholders on the deep short-, mid- and long-term implications.
- Share the concerns raised in this presentation internally in your organization and with your peers.
- Confirm that you already have ECH traffic on your network.
- Ensure that your managed endpoints disable ECH (for now).
- Configure your security stack to decrypt traffic destined to known ECH client-facing servers, effectively disabling ECH per TLS session.

Apply what you have learned in the next three to six months



In the next three to six months your enterprise should:

- Evaluate the impact of ECH on your current network security stack and DNS infrastructure:

  This should be a **joint** discussion between your network, DNS and security teams.

- Engage your legal department and regulatory compliance officers.
- Understand the broad implications on your overall security architecture:

  The paradigm shift from infrastructure layer to application layer.

- Engage your security stack vendors.

Resources

1. ECH IETF specification
   - https://datatracker.ietf.org/doc/draft-ietf-tls-esni
2. ECH white paper
   - Enterprise Strategy Group, commissioned by Symantec
   - https://docs.broadcom.com/doc/symantec-ech-whitepaper
3. ECH deployment considerations
   - https://datatracker.ietf.org/doc/html/draft-campling-ech-deployment-considerations-09
4. Inside the Internet, Duke Law Journal
   - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4466419

RSAC™ 2025 Conference

Many Voices.
One Community.